Blacklight

A Real-Time Website Privacy Inspector

By Surya Mattu

Who is peeking over your shoulder while you work, watch videos, learn, explore, and shop on the internet? Enter the address of any website, and Blacklight will scan it and reveal the specific user-tracking technologies on the site—and who's getting your data. You may be surprised at what you learn.

prudential.com
Scan Site

Visited prudential.com on Jun. 22, 2022, 16:20 ET

Learn more

Blacklight Inspection Result

Blacklight works by visiting each website with a headless browser running custom software built by The Markup. To learn more read our methodology.

26 **Ad trackers found on this site.**
This is **more than** the average of **seven** that we found on popular sites.

Websites containing advertising tracking technology load Javascript code or small invisible images that are used to either build your advertising profile or to identify you for ad targeting on this site. These techniques are often used in addition to cookies to profile you.

Blacklight detected trackers on this page sending data to companies involved in online advertising. Blacklight detected scripts belonging to **MediaMath, Inc.**, **Facebook, Inc.**, **Mouseflow**, **LinkedIn Corporation**, **Alphabet, Inc.**, **Ensighten, Inc**, **WarnerMedia, LLC**, **Demandbase, Inc.**, **Beeswax**, **Twitter, Inc.**, **TowerData, Inc.**, **Verizon Media**, **Oracle Corporation**, **Microsoft Corporation**, and **Adobe Inc.**.

How We Define This   Survey of Popular Websites

46 **Third-party cookies were found.**
This is **more than** the average of **three** that we found on popular sites.

These are commonly used by advertising tracking companies to profile you based on your internet usage.

Blacklight detected **46** third-party cookies on this site. Blacklight detected cookies set for **Microsoft Corporation**, **LinkedIn Corporation**, **Oracle Corporation**, **Demandbase, Inc.**, **Adobe Inc.**, **MediaMath, Inc.**, **Index Exchange, Inc.**, **Twitter, Inc.**, **Beeswax**, **Amobee, Inc**, **Alphabet, Inc.**, **Verizon Media**, **The Rubicon Project, Inc.**, **TowerData, Inc.**, **The Trade Desk Inc**, **WarnerMedia, LLC**, and **Bidtellect, Inc**.

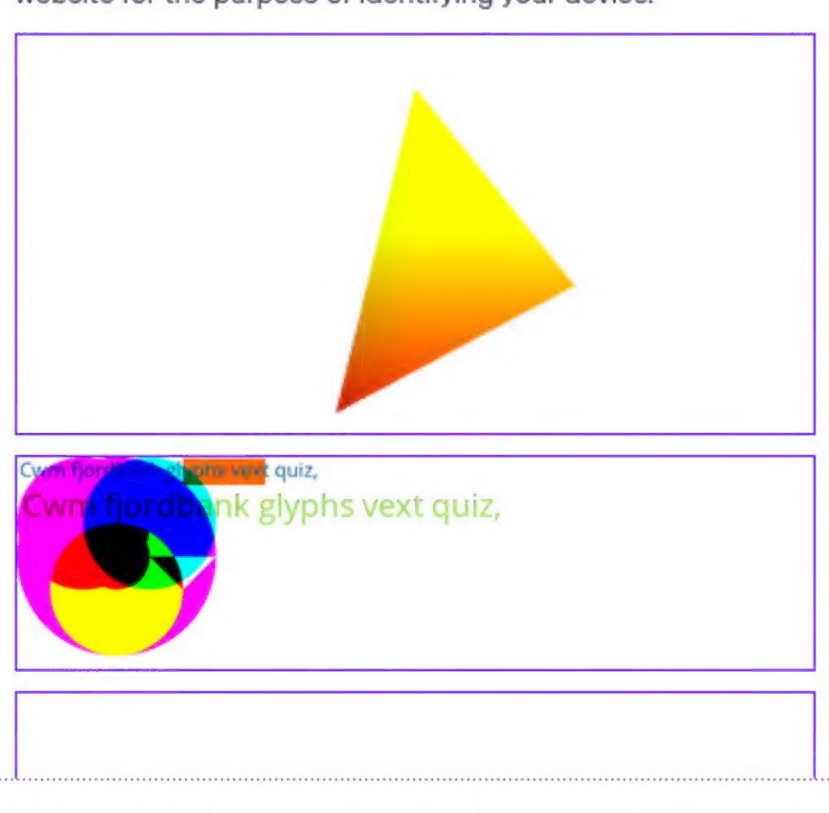
How We Define This   Survey of Popular Websites

This website loads trackers on your computer that are designed to evade third-party cookie blockers.

Canvas fingerprinting was detected on this website. This technique is designed to identify users even if they block third-party cookies. It can be used to track users' behavior across sites. This technique was used by six percent of popular sites when we scanned them in September 2020.

Blacklight detected a script loaded from **prudential.com** doing this on this site.

It secretly draws the following image on your browser when you visit this website for the purpose of identifying your device.



This website could be monitoring your keystrokes and mouse clicks.

Blacklight detected the use of a session recorder, which tracks user mouse movement, clicks, taps, scrolls, or even network activity. This data is compiled into videos and heat maps that website owners can watch to see how users interact with the site. Research has shown these practices can be insecure and make sensitive user data such as passwords and credit card information more vulnerable to leaks. This technique was used by fifteen percent of popular websites when we scanned them in September 2020.

Blacklight detected a script belonging to the company **Mouseflow** doing this on this site.

However...
While Blacklight can detect whether a session recorder was loaded, it cannot determine exactly how the collected data is being used.

How We Define This

We found this website capturing user keystrokes.

Key logging is when a website captures the text that you type into a webpage before you hit the submit button. This technique has been used to identify anonymous web users by matching them to postal addresses and real names. This technique was used by four percent of popular websites when we scanned them in September 2020.

On the site you are inspecting, information entered in the **name**, **family-name**, **given-name** fields were logged.

Blacklight detected a script loaded from **prudential.com** doing this on this site.

However...
There are other reasons for key logging, such as providing autocomplete functionality. Blacklight cannot determine the intent behind the inspected website's use of this technique.

How We Define This

When you visit this site, it tells Facebook — even if you block cookies.

The Facebook pixel is a snippet of code that sends data back to Facebook about people who visit this site and allows the site operator to later target them with ads on Facebook. A Facebook spokesperson told The Markup that the company set up this system so that a user doesn't have to be "simultaneously logged into Facebook and viewing a third-party website for our business tools to function." Common actions that can be tracked via pixel include viewing a page or specific content, adding payment information, or making a purchase. The Facebook pixel appeared in thirty percent of popular websites when we scanned them in September 2020.

This website seems to be using Facebook pixel "advanced matching" feature, which allows the site to share data about visitors with Facebook even if users block Facebook cookies.

This site sent **Email**, **First Name** and **Last Name**

How We Define This

This site allows Google Analytics to follow you across the internet.

This site uses Google Analytics and seems to use its "remarketing audiences" feature that enables user tracking for targeted advertising across the internet. This feature allows a website to build custom audiences based on how a user interacts with this particular site and then follow those users across the internet and target them with advertising on other sites using Google Ads and Display & Video 360. A Google spokesperson told The Markup that site operators are supposed to inform visitors when data collected with this feature is used to connect this browsing data with someone's real-world identity. You know when those shoes you were looking at follow you around the internet? This is one of the trackers leading to that. This feature appeared in fifty percent of popular websites when we scanned them in September 2020.

How We Define This

Some of the ad-tech companies this website interacted with:

The inspected website contacted some well known actors in the ad-tech industry. Not all of these loaded trackers, so they may be different from those listed in the tests section above. For more information on each company, what it does, and which of its domains Blacklight found during the inspection, click the arrow. Reading this can give you a better idea of how the ad-tech industry works.

Adobe

Alphabet

Blacklight detected this website sending user data to Alphabet, the technology conglomerate that encompasses Google and associated companies like Nest. The Silicon Valley giant collects data from twice the number of websites as its closest competitor, Facebook. An Alphabet spokesperson told The Markup that internet users can go here if they want to opt out of the company showing them targeted ads based on their browsing history.

The site sent information to the following domains **doubleclick.net**, **google-analytics.com**, **google.com**, **googleadservices.com**, **googleapis.com**, **googletagmanager.com**.

Company description accurate on Sept. 3, 2020   Read Google's Privacy Policy

Amazon

Blacklight detected the inspected website sending user data to Amazon, which has a wide variety of business units. The most commonly appearing Amazon trackers in our scan of popular sites in September 2020 were those for CloudFront and its marketing research arm, Alexa, which helps marketers improve their search engine performance and provides site operators insights about the popularity of their websites. (This Alexa is unrelated to Amazon's virtual assistant of the same name.) Representatives from Amazon did not respond to multiple requests for comment.

The site sent information to the following domain **amazonaws.com**.

Company description accurate on Sept. 3, 2020   Read Amazon's Privacy Policy

LinkedIn

Blacklight detected the inspected website sending user data to LinkedIn, which is owned by Microsoft. Primarily known as a career-focused social network, the company has branched out more broadly into advertising. In 2019, it purchased Drawbridge, which a company spokesperson told The Markup allows LinkedIn to "infer a member's association to their devices" in what's called an "identity graph." At the time of the acquisition, a LinkedIn executive told Ad Exchanger the company hoped Drawbridge will fill in some of the blind spots LinkedIn has on its users.

The site sent information to the following domains **adsymptotic.com**, **licdn.com**, **linkedin.com**.

Company description accurate on Sept. 3, 2020   Read LinkedIn's Privacy Policy

MediaMath

Blacklight detected the inspected website sending user data to MediaMath. MediaMath runs a "demand-side platform," which lets advertisers place ads on sites across the internet through an online portal. The company assembles profiles based on the user's previous browsing history. The company allows advertisers to target people or websites based on "aggregated, observed data on what users are browsing" on sites across the internet. A MediaMath spokesperson told The Markup that the company's service also allows advertisers to combine their data about potential customers with information collected by other ad tech companies and data brokers for more accurate ad targeting.

The site sent information to the following domain **mathtag.com**.

Company description accurate on Sept. 3, 2020   Read MediaMath's Privacy Policy

Microsoft

Blacklight detected the inspected website sending user data to Microsoft. In addition to its well-known products and services, the tech behemoth sells ads on Microsoft properties and websites that use Microsoft's search engine, Bing, for internal site searches. It also runs the Microsoft Audience Network, which uses data gathered about consumers to target ads. Of the many Microsoft-related trackers that appeared in our scan of the internet's top 80,000 most popular websites, those associated with Bing were the most common. A Microsoft spokesperson declined to tell The Markup how user data being sent to its domains was being used.

The site sent information to the following domain **bing.com**.

Company description accurate on Sept. 3, 2020   Read Microsoft's Privacy Policy

Oracle

Blacklight detected the inspected website sending user data to Oracle. Among Oracle's many different products and services is AddThis, a set of buttons that float on top of a website and allow for quick sharing on social media of the page being viewed. These buttons collect data from users and can introduce other third-party tracking technologies to a website. Oracle DMP, previously called BlueKai, helps advertisers manage the data they already have on consumers and enhance it with information acquired either from data brokers or Oracle itself—for example, linking a person to all the different devices he or she uses. An Oracle spokesperson told The Markup that the company has "actionable information" on more than a billion people.

The site sent information to the following domains **bkrtx.com**, **bluekai.com**, **eloqua.com**, **en25.com**, **maxymiser.net**.

Company description accurate on Sept. 3, 2020   Read Oracle's Privacy Policy

Magnite

Blacklight detected the inspected website sending user data to Magnite. Created by the 2020 merger of ad tech companies Rubicon Project and Telaria, Magnite places advertisements on more than million websites and apps. The company claims to have reached more than a billion consumers with ads placed on websites, mobile apps, and streaming videos. Representatives from Magnite did not respond to multiple requests for comment.

The site sent information to the following domain **rubiconproject.com**.

Company description accurate on Sept. 3, 2020   Read Rubicon Project's Privacy Policy

TowerData

Blacklight detected the inspected website sending user data to Tower Data, an ad tech company that creates profiles of web users anchored to their email address, according to its website. It also sells data about voters to political campaigns. Representatives from Tower Data did not respond to multiple requests for comment.

The site sent information to the following domain **rlcdn.com**.

Company description accurate on Sept. 3, 2020   Read TowerData's Privacy Policy

Verizon

Blacklight detected the inspected website sending user data to Verizon. While best known for providing cellphone and broadband service, Verizon has gained a significant presence in online advertising through acquisitions of ad-focused companies like AOL and Yahoo!, which offer advertising services in addition to content. Domains associated with Yahoo! and AOL (specifically, advertising.com, which was part of AOL before Verizon's purchase of the company) appeared the most frequently among the many Verizon-controlled trackers appearing in our scan of popular websites in September 2020. Representatives from Verizon did not respond to multiple requests for comment.

The site sent information to the following domain **yahoo.com**.

Company description accurate on Sept. 3, 2020   Read Verizon's Privacy Policy

See Something Worrying?   Tell us about it

Blacklight results should not be taken as the final word on potential privacy violations by a given website. Rather, they should be treated as an initial automated inspection that requires further investigation before a definitive claim can be made.

DuckDuckGo's Tracker Radar last updated Sept. 3, 2020. For more information on how we use it, read our methodology.

Concept and development
Surya Mattu

Design and front-end development
Sam Morris

Infrastructure and security
Simon Fondrie-Teitler

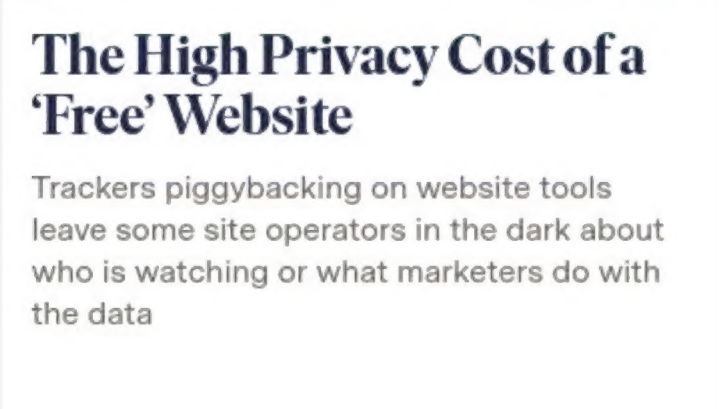
Research and reporting
Aaron Sankin

Editing
Evelyn Larrubia

Copy editing
Jill Jaroff

Initial platform development
Yotam Mann and Chris Deaner

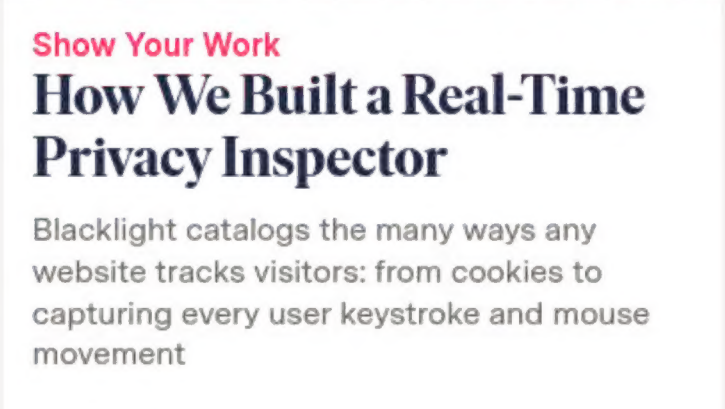
More on Blacklight



The High Privacy Cost of a 'Free' Website

Trackers piggybacking on website tools leave some site operators in the dark about who is watching or what marketers do with the data

September 22, 2020 08:00 ET

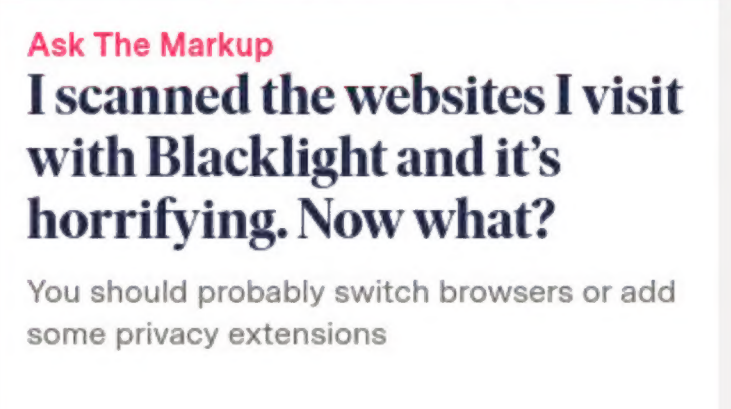


Show Your Work

How We Built a Real-Time Privacy Inspector

Blacklight catalogs the many ways any website tracks visitors: from cookies to capturing every user keystroke and mouse movement

September 22, 2020 08:00 ET



Ask The Markup

I scanned the websites I visit with Blacklight and it's horrifying. Now what?

You should probably switch browsers or add some privacy extensions

September 22, 2020 08:00 ET